

REMARKS

In the Final Office Action mailed on October 5, 2004, all pending claims 1-27 were rejected by the Examiner. Applicant respectfully traverses the rejections and requests reconsideration of the present application in view of the arguments below.

Rejections Under 35 U.S.C. §§ 102 and 103

In the Final Office Action, the Examiner rejected each of the independent claims 1, 14 and 27 under the same proposed combination of prior art utilized in the previous Office Action mailed on March 16, 2004. Specifically, the Examiner rejected claims 1, 2, 5, 8, 10-17, 19 and 27 under 35 U.S.C. § 102 (b) as being anticipated by U.S. Patent No. 5,823,948 to Ross, Jr. et al., which is herein referred to as the “Ross” reference. In addition, the Examiner rejected claims 3, 4, 6, 7, 9, 18 and 20-26 under 35 U.S.C. § 103(a) as being unpatentable over the Ross reference in view of U.S. Patent No. 5,960,406 to Rasansky et al., which is herein referred to as the “Rasansky” reference. Again, Applicant respectfully traverses these rejections.

As the Examiner has merely repeated the rejections from the previous Office Action mailed on March 16, 2004, the Applicant will address assertions made in the Response to Argument section, which are believed to crystallize the Examiner’s position. As such, the arguments, which were presented in the previous Response to Office Action mailed on March 16, 2004, are hereby incorporated by reference. Accordingly, the Applicant again respectfully requests withdrawal of the rejections and allowance of pending claims 1-27.

Examiner’s Assertions in the Response to Arguments Section

In the Final Office Action, the Examiner made various assertions regarding the rejections, which were formulated in the Response to Argument section. Applicant respectfully traverses these assertions, and will address specific assertions that appear to crystallize the Examiner’s position. First, Applicant traverses the Examiner’s assertions that the recitations of storing data for a user *in space inaccessible to the user*, which are recited in

the independent claims 1, 14, 20 and 27, are disclosed or even suggested in the passages cited by the Examiner in the Ross reference. Secondly, Applicant traverses the Examiner's assertions that the recitations of *accessing data to create a secure data file*, which are recited in the independent claims 1, 14 and 27, are disclosed or even suggested in the passages cited by the Examiner in the Ross reference. Finally, Applicant traverses the Examiner's assertions that relate to the alleged motivation for the combination of the Ross reference with the Rasansky reference. Hence, the Examiner's assertions do not support the rejections.

As a preliminary matter, it should be noted that the present application describes that secure collection and storage of sensitive data for reporting purposes is a concern to users because of unauthorized access to the data. In particular, the present technique utilizes a separate processing space to store data, which is secure and not accessible to users, such as the user who entered or is destined to receive the report. *See id.* at page 3, lines 22-27. The recitations of *storing data for a user in space inaccessible to the user* and *accessing data to create a secure data file* are clearly recited in the independent claims 1, 14, 20 and 27. Specifically, independent claim 1 recites:

storing data for a user on a secure data repository and
operative in a first processing space inaccessible to the user;
accessing data from the repository to create a secure data file
in the first processing space. (Emphasis added).

Independent claim 14 recites:

storing user data associated with the user in a first data
repository;
transmitting at least a portion of the user data from the first
data repository to a second data repository operative in a first
processing space inaccessible to the user;
...
exporting the secure data file to a second processing space
separated from the first processing space and accessible to the user.
(Emphasis added).

Further, independent claim 20 recites:

a secure data repository operative in a first processing space for storing user data input via a configurable network, *the first processing space being inaccessible by the user* via the network;
a data access program module, operative in the first processing space for extracting report data from the secure data repository;
a second data repository operative in a second processing space securely separated from the first processing space for storing the report data extracted by the data access program module.
(Emphasis added).

Finally, independent claim 27 recites:

means for storing data for a user on a secure data repository and operative in a first processing space inaccessible to the user;
means for accessing data from the repository to create a secure data file in the first processing space. (Emphasis added).

Hence, each of the independent claims 1, 14, 20 and 27 relates to storing data for a user *in space inaccessible to the user*, and each of the claims 1, 14 and 27 relates to *accessing data to create a secure data file*.

With regard to the first point, the Examiner asserted that certain passages of the Ross reference disclose a first processing space inaccessible to the user. In an attempt to support this assertion, the Examiner relied upon two passages, at col. 5 lines 5-10 and 34-52 of the Ross reference. Specifically, the Examiner asserted that these passages teach “storage of data on communication and file servers” and “a secure data repository operative for storing user data input.” See Office Action mailed October 5, 2004, pp. 3-4. Yet, the passages and even the Examiner’s assertions do not address the fact that the claims recite that the *first processing space is inaccessible to the user* because other recitations relate to the user being on a configurable network. Specifically, the passages relied upon by the Examiner state:

The transcribed dictations are placed in an electronic storage bin in the communications server(s) for transferring the dictation transcriptions to the file servers, and storing the dictation transcriptions in the file servers 2 and 3 as text associated with patient data for particular patients.

...

The patient record documentation method provides tracking and order entry. File servers provide data and software from the file servers through a network hub and network to multiple CPU'S. The patient data is transferred from the CPU's to the file servers. Portions of the record that are unique to particular patients are dictated. The dictation is transmitted over voice lines to a transcription center where the dictation is transcribed. The transcribed dictation is transmitted to the communication server(s), which feeds the dictation transcription to the file servers as text components. The text on particular patients is stored in the file server with the tabled data. Word and sentence generation and coordination software is stored in the peripheral CPU'S. Monitors display text sentences generated by the generation software as summaries, together with the text from the dictation transcriptions. The text summaries are sent from the peripheral CPU's to a printer via the local network for generation of printed patient textual reports with sentences generated in medical English text.

Ross, Jr. et al., col. 5, lines 5-10 and 34-52.

These passages disclose that transcribed dictations are stored with other files in the file servers 2 and 3. *See id.* Any personnel on the network may track and order these files from the file servers. *See id.* The access to the network, as described in other passages, is only limited to personnel that demonstrate their identity to establish access to the network with specific rights in the network. *See* Ross, col. 12, lines 55-67. That is, the only limitation in access to the patient data is the modification of the patient data, which is limited to personnel who are in a certain class of users, such as the personnel that entered the data. *See id.* at col. 13, lines 5-31. As such, any user able to connect to the network is able to access these files.

These teachings are contrary to the claim recitations because the claims require that the data is stored for the user in a *first processing space that is inaccessible* to the user. The Examiner appears to assert that denial of access to a user to the network satisfies this recited feature. However, the mere limitation of access to the network does not provide the *first processing space that is inaccessible* to the user because other recitations in the claims provide that the user is on the network to receive other information, such as the report that is based on the data stored in the first

processing space. As a result, the Ross reference does not disclose or teach storing data in a processing space that is *inaccessible to the user* because any personnel can access the patient data and the personnel that entered the data can view and modify the data. As such, the Examiner's assertions are clearly not supported by the Ross reference and do not anticipate the claim subject matter.

With regard to the second point, the Examiner asserted that the above cited passages of the Ross reference disclose *accessing data to create a secure data file*. In particular, the Examiner asserted that these passages teach this recitation, but the Examiner failed to allege or particularly point to any specific structures or elements that disclose the *secure data file*. See Office Action mailed October 5, 2004, p. 3. Accordingly, when properly construing the claims in view of the previous discussion, Applicant submits that no structures in the Ross reference correspond to the *secure data file* because the Ross reference does not disclose or suggest any secure files. That is, the Ross reference merely describes that patient data is transferred from the CPU's, which are the peripheral devices 9, to the file servers 2 and 3. See *id.* at col. 5, lines 34-46. The patient data, which may include transcriptions of dictations in the form of text files along with other patient data, is accessible by the user. Because other recitations in the claims provide for the user being on the network, the mere limitation of access to the network does not provide the secure data file. As a result, the Ross reference does disclose or teach creating a secure data file because any personnel can access the patient data. As such, the assertions are clearly not supported by the Ross reference. The reference, therefore, cannot anticipate the claimed subject matter.

Finally, with regard to the third point, Applicant will address the Examiner's rationale for combining the references, although Applicant does not believe that the combination of the Ross and Rasansky references would or could include all of the recited features, as discussed in the previous response to Office Action. The Examiner's rationale for combining the references appears to be based on potential advantages hypothesized by the Examiner, not on the teachings in references themselves or any other *evidence* found in the art. In the rejection, the Examiner asserted that the combination is obvious because one

of ordinary skill in the art would modify the system of Ross by storing the report template in the second processing space to reduce the time required to generate a report by eliminating the step of transferring the report template data to the second processing space. However, this statement is nothing more than an assertion, which is not supported by any evidence of record. The Examiner has not provided any *evidence* of suggestion by the prior art references that the proposed advantages would be expected from the combination. Accordingly, because no teaching or suggestion supporting the combination is present, the Examiner's proposed combination is unsupported speculation and therefore is not proper.

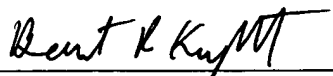
For at least these reasons, independent claims 1, 14, 20 and 27, and the respective dependent claims are believed to be allowable over the Ross reference, alone or in combination with the Rasansky reference. Therefore, withdrawal of the rejections and allowance of the claims is respectfully requested.

Conclusion

In view of the remarks set forth above, Applicant respectfully requests allowance of pending claims 1-27. If the Examiner believes a telephonic interview will help speed this application towards issuance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Date: December 6, 2004



Brent R. Knight
Reg. No. 54,226
FLETCHER YODER
P.O. Box 692289
Houston, TX 77269-2289
(281) 970-4545